Ahmad Yousuf

Portfolio Project 3

08/02/2025

Incident Response Playbook Development

Objective

Develop a structured incident response playbook outlining detection, containment, and recovery procedures for phishing and malware threats.

Background and Motivation

Incident response playbooks provide repeatable procedures for handling security incidents. They reduce response time, improve consistency, and support compliance. This project focused on building playbooks for two common threats: phishing and malware infections.

Scope

- Covered phishing and malware scenarios
- Defined detection, containment, and recovery steps
- Targeted small to mid-sized enterprise environments
- No live incident simulation or automation included

Tools and Technologies

- MITRE ATT&CK Framework
- NIST SP 800-61
- Splunk
- Microsoft Defender
- Markdown or Excel for documentation

Phishing Response Summary

Detection

- Indicators: suspicious emails, credential harvesting, unusual logins

- Sources: email logs, endpoint logs, authentication logs
- Actions: search for phishing domains, monitor login anomalies

Containment

- Block sender and URLs
- Isolate affected endpoints
- Disable compromised accounts

Recovery

- Remove malicious emails
- Reset credentials
- Validate cleanup and educate users

Malware Response Summary

Detection

- Indicators: unknown processes, malicious connections, file changes
- Sources: endpoint protection, Sysmon, firewall logs
- Actions: search for malware signatures, monitor process behavior

Containment

- Disconnect infected systems
- Suspend user accounts
- Block malicious traffic

Recovery

- Remove malware or reimage systems
- Restore from backups
- Validate cleanup and monitor for persistence

Challenges and Solutions

- Standardizing procedures across threats required modular templates
- Scope was kept narrow to maintain clarity
- Mapped steps to available tools for operational feasibility

Security Considerations

- Playbook assumes basic log and endpoint visibility
- Designed for manual response workflows
- Emphasizes documentation and validation

Conclusion

This project produced a usable incident response playbook for phishing and malware threats. It supports consistent and effective response and can be expanded to cover additional scenarios or integrate automation.

References

- NIST SP 800-61: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- MITRE ATT&CK: https://attack.mitre.org
- Microsoft Defender: https://learn.microsoft.com/en-us/microsoft-365/security
- Splunk Security Use Cases: https://www.splunk.com/en_us/solutions/security.html